AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for message authentication, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

employing a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

employing a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, employing a the private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient.

2. (Previously presented) The method of Claim 1, further comprising a text record that is accessible to the DNS and which includes at least the public component of the key pair.

3. (Original) The method of Claim 1, further comprising generating a selector that is associated with the key pair, wherein the selector is employable to identify the key pair's public component for accessing by the DNS.

4. (Original) The method of Claim 3, further comprising forming a lookup query for the DNS by combining the selector with the sender's address.

5. (Currently amended) The method of Claim 1, wherein the message server includes ~~further comprising employing~~ a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

6. (Currently amended) The method of Claim 1, wherein the message server includes ~~further comprising employing~~ a mail server associated with the domain to employ the private component of the key pair to digitally sign the message.

7. (Currently amended) The method of Claim 1, wherein the message server includes ~~further comprising employing~~ a mail server that is associated with ~~a~~ the domain of the recipient to verify the domain of origination for the message with the public component of the key pair.

8. (Currently amended) The method of Claim 1, wherein the message server includes ~~further comprising employing~~ a mail server that is associated with ~~a~~ the domain of the recipient to provide the verified digitally signed message to the recipient.

9. (Original) The method of Claim 1, further comprising accessing the public component of the key pair by employing a text record in a look up table for the DNS.

10. (Original) The method of Claim 1, further comprising generating a plurality of key pairs associated with the domain, wherein at least two key pairs are associated with at least two different senders and wherein each public component of each key pair is accessible by the DNS associated with the domain.

11. (Original) The method of Claim 10, further comprising separately associating private components of the at least two key pairs with at least two mail servers, wherein the at least two mail servers are associated with the domain.

12. (Original) The method of Claim 10, wherein each private component of each key pair employs a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

13. (Original) The method of Claim 1, further comprising employing one of a plurality of mail servers associated with the domain to digitally sign the message with the private component of the key pair and forward the digitally signed message towards the recipient.

14. (Original) A system for message authentication, comprising:

a client that is enabled to generate at least one message for a recipient, wherein the client is associated with a domain;

a mail server associated with the domain of the client, wherein the mail server performs actions, including:

enabling the generation of a key pair associated with the domain, wherein a public component of the key pair is accessible to a DNS that is associated with the domain; and

if a message from the client originates from the domain, enabling a private component of the key pair to digitally sign the message and forward the digitally signed message towards the recipient of the message; and

a mail server associated with a domain of the recipient, wherein the mail server performs actions including enabling the public component stored with the DNS to verify that the digitally signed message originated from the domain associated with the client, and enabling each verified digitally signed message to be provided to the recipient.

15. (Original) The system of Claim 14, wherein the message is at least one of an email, instant message (IM), short message service (SMS).

16. (Original) The system of Claim 14, further comprises a text record that is accessible to the DNS and which includes at least the public component of the key pair.

17. (Original) The system of Claim 14, further comprises a selector that is associated with the key pair, wherein the selector is employable to identify the key pair's public component for accessing by the DNS.

18. (Original) The system of Claim 14, further comprising a plurality of key pairs that are associated with at least two different clients, wherein each public component of each key pair is accessible by the DNS associated with the domain.

19. (Currently amended) A ~~carrier wave signal~~ processor readable medium of tangibly embodied software that enables actions for message authentication, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

enabling a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, employing ~~a~~ the private component of the key pair to digitally sign the message and forwarding the digitally signed message towards ~~a~~ the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient.

20. (Currently amended) The processor readable medium ~~carrier wave signal~~ of Claim 19, further comprising generating a selector that is associated with the key pair, wherein the selector is employable to identify the key pair's public component for accessing by the DNS.

21. (Currently amended) The processor readable medium ~~carrier wave signal~~ of Claim 19, further comprising generating a plurality of key pairs associated with the domain, wherein at least two key pairs are associated with at least two different senders and wherein each public component of each key pair is accessible by the DNS associated with the domain.

22. (Currently amended) The processor readable medium ~~carrier wave signal~~ of Claim 21, further comprising separately associating private components of the at least two key pairs with at least two mail servers, wherein the at least two mail servers are associated with the domain.

23. (Currently amended) The processor readable medium ~~carrier wave signal~~ of Claim 21, wherein each private component of each key pair employs a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

24. (Currently amended) A client that enables message authentication, comprising:

a first component for originating a message for communication by a message server associated with a domain, wherein ~~the generation of a~~ key pair is associated with ~~a~~ the domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

a second component for enabling the message server associated with the domain to employ a private component of the key pair to digitally sign the originated message;

a third component for enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, a fourth component that provides for enabling a private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, a fifth component for providing the verified digitally signed message to the recipient.

25. (Original) The client of Claim 24, further comprising enabling the generation of a plurality of key pairs associated with the domain, wherein at least two key pairs are associated with at least two different senders and wherein each public component of each key pair is accessible by the DNS associated with the domain.

26. (Original) The client of Claim 25, further comprising enabling the separate association of private components of the at least two key pairs with at least two mail servers, wherein the at least two mail servers are associated with the domain.

27. (Original) The client of Claim 25, further comprising enabling each private component of each key pair to employ a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

28. (Currently amended) A message server that enables message authentication, comprising:

a first component for enabling the generation of a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

wherein the message server is associated with the domain and employs a private component of the key pair to digitally sign a message that is originated with the message server;

a second component for enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, a third component for enabling a the private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards a the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, a fifth component for providing the verified digitally signed message to the recipient.

29. (Currently amended) A method for enabling message authentication, comprising:

means for enabling the generation of a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

means for employing a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

means for employing a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, means for enabling a private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, means for providing the verified digitally signed message to the recipient.